We're going compute some DSA examples, except with smaller values for p and q.

For the hash function, we'll use SHA3-256. You will want to grab the Mathematica notebook for today to see the syntax for computing the hash value.

1. Alice publishes $(p, q, \alpha, \beta) = (241\,553\,623, 13\,033, 52\,824, 238\,101\,207)$

   (a) Given that we're using smaller values, verify that p, q and α are reasonable choices.

   (b) Which, if any, of the following are valid DSA signatures?
   (Don't include the quotation marks when calculating the hash.)

      i. $(x,\ (r, s)) =$ ("Argybargy", $(5105, 11\,671)$)

      ii. $(x,\ (r, s)) =$ ("Pleased to Meet Me", $(9543, 3174)$)

2. You want to use DSA to sign the message

   "Clam chowder is just hot ocean milk with dead animal croutons"

   using values of

   $$p = 2\,738\,078\,869, \qquad q = 65\,323, \qquad \text{and } \alpha = 11\,208$$

   (a) Verify that p, q and α are reasonable choices.

   (b) Use $d = 17\,132$ to compute your value for β.

   (c) Use a value of $k_E = 41\,821$ to sign your message.

3. When using DSA to sign a message, you compute $r \equiv \left(\alpha^{k_E} \mod p\right) \mod q$.

   Does it matter whether you first reduced mod q and then mod p or reduce in the other order?

   In other words, is $\left(\alpha^{k_E} \mod p\right) \mod q$ equal to $\left(\alpha^{k_E} \mod q\right) \mod p$?